Nationaal Lucht- en Ruimtevaartlaboratorium

National Aerospace Laboratory NLR

NLR-TP-2002-281

Secure Meta-computing in an Extended Enterprise

B.C. Schultheiss, L.C.J. van Rijn and C. Kamphuis

Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2002-281

Secure Meta-computing in an Extended Enterprise

B.C. Schultheiss, L.C.J. van Rijn and C. Kamphuis

This report is based on a presentation held at ICE2002, Rome, Italy, 17-19 June 2002.

Customer:	National Aerospace Laboratory NLR
Working Plan number:	I.2.A.4
Owner:	National Aerospace Laboratory NLR
Division:	Information and Communication Technology
Distribution:	Unlimited
Classification title:	Unclassified
	May 2002

Summary

A shared design environment enables companies in an Extended Enterprise to view available data and applications, and to easily access them. A key factor for such a design environment is security, obeying the business rules of companies. The solution for such a design environment presented in this paper applies a security approach based upon the developments in the EU project ENHANCE, and SPINEware to facilitate the implementation of the meta-computing environment. A workflow from the EU project ASICA is used to illustrate the usage of such an environment.

Contents

2 Figures

(10 pages in total)

Abbrevations

ASICA	Air Management Simulation for Aircraft Cabins
EE	Extended Enterprise
ENHANCE	ENHanced AeroNautical Concurrent Engineering
EU	European Union
HTTP	Hyper Tekst Transmission Protocol
HTTPS	Hyper Tekst Transmission Protocol, Secure
IPSec	Secure IP Protocol
IT	Information Technology
PZ	Project Zone
VPN	Virtual Private Networks

1 Introduction

In an Extended Enterprise (EE) collaboration is an important issue and companies only participate if certain conditions are met. Using the knowledge and expertise of different companies implies sharing of computing resources and distributed use of software applications. Some software applications may require specific high performance computing facilities, whilst others require dedicated graphical devices. Also, applications may only run on an appointed host due to licensing restrictions or cost effectiveness. Current technology supports use of distributed facilities, and customers expect this as a minimum.
The companies in the EE need to know which applications and data are available, and should be able to easily access them. A shared design environment would show the companies the tools and data that can be accessed. Such a shared environment crosses borders of companies, which requires measures with respect to security. The end-user of such a design environment should be able to access the applications and data without being confronted with low-level details emerging from the underlying computing system and networks, such as conversions, transfers of files, and location of applications. This transparent distributed access is also known as meta-computing.

2 The approach using existing theories and work

The approach for implementing a secure meta-computing environment for an EE is a combination of the developments in the EU project ENHANCE, and applying SPINEware as a middleware system to construct a working environment on top of the secured environment.

2.1 Security

ENHANCE - ENHanced AeroNautical Concurrent Engineering is a large European project that aims at defining new common ways of working, with related operational development tools, engineering methods and organisational guidelines for joint European aeronautics product development. It provides concurrent engineering methods and tools for the European aircraft industry, including aeronautical research centres, and airlines.
One of the ENHANCE work packages focuses on secure, reliable communication among partners of the EE over an insecure network. The Internet was chosen as the medium to interconnect the organisations involved within an EE. The problem to be solved was enabling global connectivity through the Internet, whilst protecting the information on the resulting joint network. The most characteristic aspects of the ENHANCE IT Security Approach are the Virtual Private Network (VPN [Scott, Wolfe and Erwin, 1999]) and the Project Zone (PZ).

VPNs are encrypted connections that enable the secure transfer of private data over the Internet. These connections cannot be monitored by third parties. The IT Security approach connects PZs of the Extended Enterprise organisations through VPNs based on IPSec [IPSec, 1998]. Also secure HTTP (HTTPS), or setting up connections through the secure shell SSH could be applied. An advantage of VPNs is that they can be installed independently from the application using it. Whereas applying HTTPS means that the client-server application must support HTTPS.

A PZ is a zone within an enterprise having its own project specific security measures. Within the EE, connections to a project zone are only allowed from “trusted” local network connections and from “trusted” connections from the VPN. Servers and applications that are shared within the EE, must be hosted within PZs, thus enabling secure sharing, without enabling outside access to the private networks (see Fig. 1).

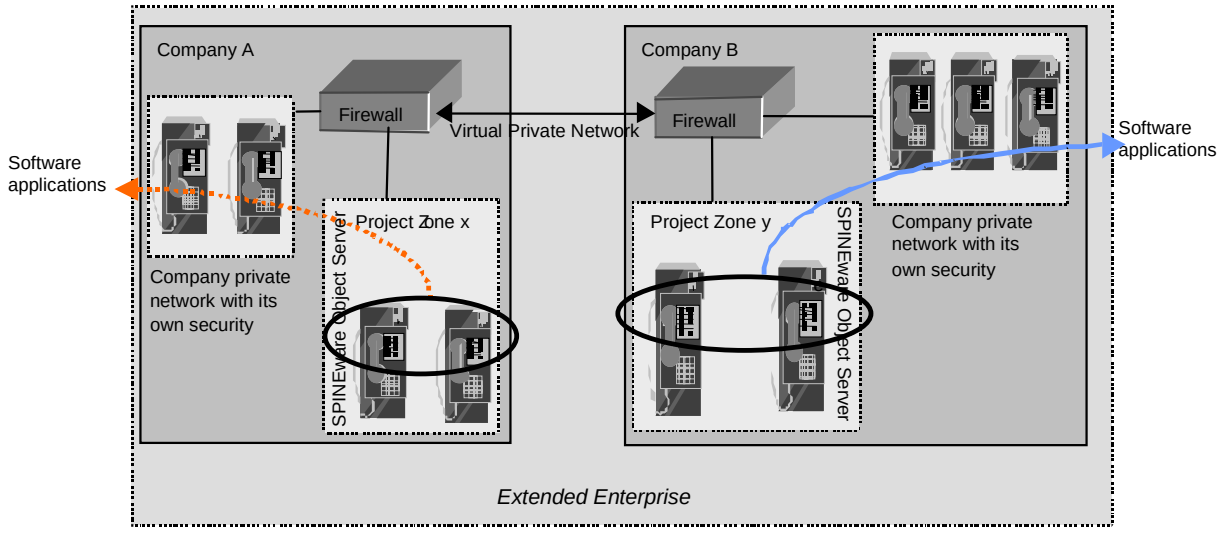

Fig. 1 Meta-computing through VPNs and PZs in an Extended Enterprise

2.2 Meta-computing

Meta-computing refers to a uniform and network transparent access to the resources and applications available from the computer network. The meta-computing environment is constructed using SPINEware. SPINEware is a middleware system that supports the construction and usage of working environments on top of existing networks [Baalbergen, van der Ven, 1999]. In this case, the existing network consists of companies connected through VPNs (see Fig. 1).

Through SPINEware, an end user has access to a single application environment - a meta-computer - providing uniform and network transparent access to the resources and applications available from the computer network. This design environment can be accessed using a locally installed SPINEware browser, or through a web-browser [Schultheiss, Baalbergen, 2001]. Using the design environment, the user can browse local and remote information, start tools, and submit jobs, using point-and-click and drag-and-drop operations.
SPINEware offers the possibility of constructing a workflow object, in which tools can be chained. Using workflows provides insight into the (progress of the) process flow, and enables automatic execution of tools, even if these tools are physically located on various hosts.

3 Illustration using an ASICA workflow

The SPINEware approach has been proven to be successful in various projects. It has been applied as part of the ENHANCE heterogeneous workflow demonstrator. In this section, it is explained how PZs and VPNs are applied to secure an existing SPINEware meta-computing environment. This will be illustrated using a workflow developed in the ASICA project. First the ASICA workflow is explained, next the security approach is described.
ASICA – Air Management Simulation for Aircraft Cabins – is a European project carried out by a consortium that consists of eleven European companies, aiming at the improvement of air conditioning systems on board aircraft. ASICA applies SPINEware to construct the design environment for accessing central resources through a web interface. The simulation tools are physically located in NLR's working environment on various hosts. Execution is started from and end user's local site.

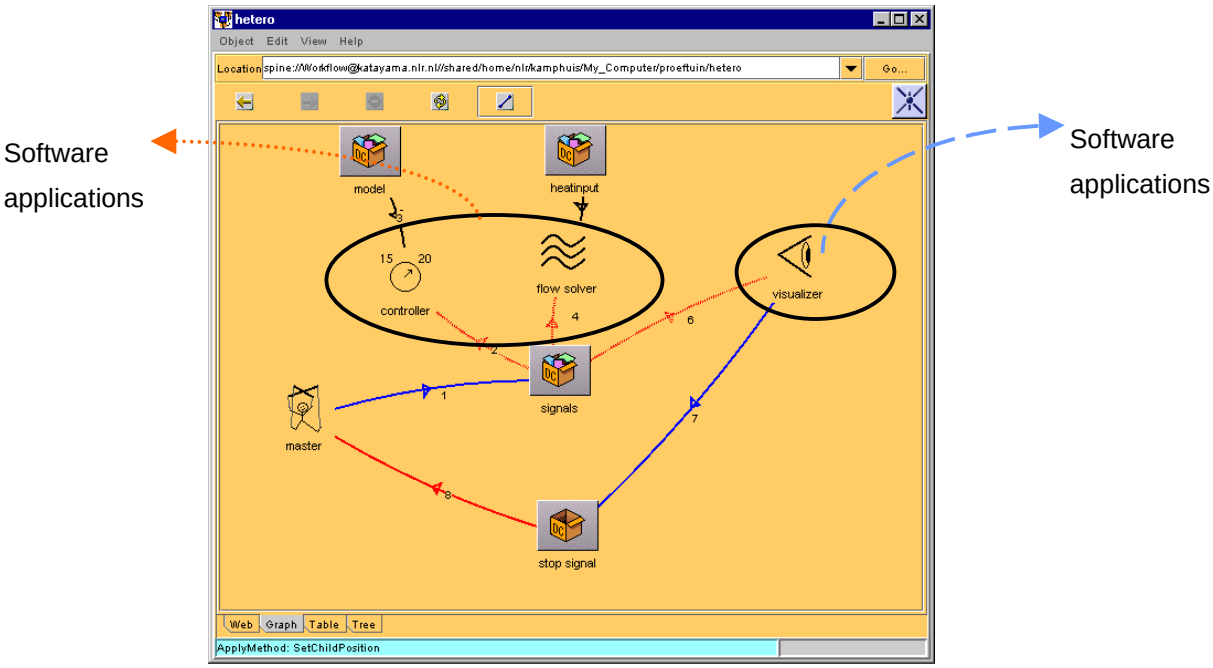

Fig. 2 A distributed workflow

To automate the execution of tools and transfer of files, a workflow consisting of chained distributed tools is defined (see Fig. 2). The goal of the presented workflow is to evaluate controller designs by visualisation of the aircraft cabin flow. The workflow comprises three tools: Flow solver, Controller, and Visualiser. It concerns the co-simulation of the time-dependent behaviour of the airflow in the cabin and a controller of the cabin air supply. The control is based on measurements of the cabin temperature. The time-dependent behaviour of the cabin flow is simulated through Computational Fluid Dynamics techniques that are applied to the time-dependent turbulent incompressible Navier-Stokes equations.

Initially, the software applications in the ASICA workflow are distributed over NLR hosts only, and the environment is accessed through a web interface. When we move the visualisation to a partner's local workstation, SPINEware will take care of launching the visualisation on this local work-station, including the transfer of files from and to the correct locations. Since this communication takes place over the Internet, secure communication is desirable. The ASICA PZ at NLR can easily be configured to accept a VPN connection with the local workstation. The necessary communication between the visualiser application and the simulation takes place via this VPN.

From low level point of view, transparently to end users, meta-computing object servers (SPINEware object servers) are running on the local work station and in the ASICA PZ at NLR. These object servers take care of handling requests on e.g. workflows, files, and tools, or they forward the request to for example the object server that takes care of launching the

visualisation tool. The object servers communicate with each other through the VPNs. The servers are started automatically by the SPINEware web server, or by already started object servers whenever required. So, for example the object server running on the local workstation takes care of starting the visualisation tool, including data transfers.

4 Findings

Within the ENHANCE project, VPNs have already been successfully applied to secure the communication among various applications which are hosted by distributed sites and interconnected via the Internet. VPNs were recognised as flexible and reliable solutions for meeting the security requirements for virtual and mobile teams in an EE. One of the advantages of the Internet approach is that it significantly reduces the costs for communication.
Results from the ASICA project are the ASICA design environment as constructed with SPINEware. By defining and using a workflow to execute a simulation run, knowledge is preserved within the design environment. This domain knowledge is transferred from tacit into explicit knowledge, and as such competence management is supported. This workflow is accessible by ASICA partners, and can be reused many times. The familiarisation effort for new employees is reduced by this working method. Another result is that the design environment promotes the use of project standards, and project standard tools. The PZs with VPN connections approach shows that the ASICA design environment could be secured, resulting in SPINEware object servers located in different PZs communicating over VPNs.

5 Conclusions

The design environment supported by SPINEware provides users easy access to data and chains of tools distributed over the EE. Engineering process flows, tools and data are stored into this meta-computing environment by the participating companies. The application of VPN and PZs assures the security of the meta-computing environment.

6 Acknowledgement

The ASICA project is partly funded by the EC in the Growth programme. The ENHANCE project is partly funded by the EC. The paper does not represent the view of the EC, and the authors solely are solely responsible for the paper’s contents.

7 References

1. ASICA: http://www.asica.fr.st, the ASICA website.
2. Baalbergen, E.H.; Ven, H. van der; *SPINEware, a framework for user-oriented and tailorable metacomputers*, in: Future Generation Computer Systems 15 (1999) pp. 549-558, NLR-TP-98643.
3. ENHANCE: http://www.enhanceproject.com, the ENHANCE web-site.
4. Heerema, F.J.; Posthuma de Boer, U. (ed.); *The Road to the Virtual Enterprise, ICT in aerospace research and development*, National Aerospace Laboratory NLR, April 2001, ISBN 90-806343-1-x.
5. IPsec: RFC 2401, *Security Architecture for the Internet Protocol*, 1998, http://www.rfc-editor.org.
6. Scott, C.; Wolfe, P.; Erwin, M.; *Virtual Private Networks*, second edtion, January 1999, O'Reilly & Associates, ISBN 1-56592-529-7.
7. Schultheiss, B.C.; Baalbergen, E.H.; *Utilizing supercomputer power from your desktop*, HPCN 2001 proceedings in the Springer Verlag series Lecture notes in Computer Science, NLR-TP-2001-181.